TechXplore

# Vulnerabilities of electric vehicle charging infrastructure

November 15 2022

Kaedi Sanchez plugs in her car at a City of Albuquerque electric vehicle charger before heading to work. Sandia National Laboratories researchers have been studying the vulnerabilities of electric vehicle charging infrastructure, including public chargers, to better inform policymakers. Credit: Craig Fritz

With electric vehicles becoming more common, the risks and hazards of a cyber attack on electric vehicle charging equipment and systems also increases. Jay Johnson, an electrical engineer at Sandia National Laboratories, has been studying the varied vulnerabilities of electric vehicle charging infrastructure for the past four years.

Johnson and his team recently published a summary of known electric vehicle charger vulnerabilities in the journal *Energies*.

"By conducting this survey of electric vehicle charger vulnerabilities, we can prioritize recommendations to policymakers and notify them of what security improvements are needed by the industry," Johnson said.

"The Bipartisan Infrastructure Law allocates $7.5 billion to electric vehicle charging infrastructure. As a part of this funding, the federal government is requiring states to implement physical and cybersecurity strategies. We hope our review will help prioritize hardening requirements established by the states. Our work will also help the federal government standardize best practices and mandate minimum security levels for electric vehicle chargers in the future."

## Compiling vulnerabilities

Electric vehicle charging infrastructure has several vulnerabilities ranging from skimming credit card information—just like at conventional gas pumps or ATMs—to using cloud servers to hijack an entire electric vehicle charger network.

Sandia researchers are working with experts from Argonne, Idaho and Pacific Northwest national laboratories; the National Renewable Energy Laboratory; and others as a national security laboratories team.

"We are focused on larger impacts to critical infrastructure as we electrify more of the transportation industry," Johnson said. "We have been studying potential impacts to the power grid. Also, as law enforcement and other government agencies consider switching to electric vehicles, we've been thinking about how the inability to charge vehicles could impact operations."

Brian Wright, a Sandia cybersecurity expert on the project, agreed about the scale of the challenge.

"We don't want bad things to happen to the grid, and we want to keep electric vehicle drivers safe and protect people working on the equipment," Wright said.

"Can the grid be affected by electric vehicle charging equipment? Absolutely. Would that be a challenging attack to pull off? Yes. It is within the realm of what bad guys could and would do in the next 10 to 15 years. That's why we need to get ahead of curve in solving these issues."

The team looked at a few entry points, including vehicle-to-charger connections, wireless communications, electric vehicle operator interfaces, cloud services and charger maintenance ports. They looked at conventional AC chargers, DC fast chargers and extreme fast chargers.

The survey noted several vulnerabilities on each interface. For example, vehicle-to-charger communications could be intercepted and charging sessions terminated from more than 50 yards away. Electric vehicle owner interfaces were chiefly vulnerable to skimming of private information or changing charger pricing.

Most electric vehicle chargers use firewalls to keep separate from the internet for protection, but Argonne National Laboratory researchers found some systems did not. Additionally, an Idaho National Laboratory team found some systems were vulnerable to malicious firmware updates.

The multi-lab team found many reports of charger Wi-Fi, USB or Ethernet maintenance ports allowing reconfiguration of the system. Local access could allow hackers to jump from one charger to the whole charger network through the cloud, Johnson said.

## Patches and next steps

In the paper, the team proposed several fixes and changes that would make the U.S. electric vehicle charging infrastructure less vulnerable to exploitation.

These proposed fixes include strengthening electric vehicle owner authentication and authorization such as with a Plug-and-Charge public key infrastructure, Johnson said. They also recommended removing unused charger access ports and services and adding alarms or alerts to notify charger companies when changes are made to the charger, like if the charger cabinet is opened.

For the cloud, they recommended adding network-based intrusion detection systems and code signing firmware updates to prove that an update is authentic and unmodified before being installed. Sandia has produced a best-practices document for the charging industry.

Now that this review has been completed, the Sandia team has received follow-on funding to tackle some of these gaps. They are working with Idaho and Pacific Northwest national laboratories to develop a system for electric vehicle chargers. This system will use cyber-physical data to prevent bad guys from impacting the electric vehicle charging infrastructure.

The team has another research project that involves evaluating public key infrastructures for electric vehicle charging, providing hardening recommendations for charging infrastructure network owners, developing electric vehicle charging cybersecurity training programs and assessing the risk of the various vulnerabilities. Risk analysis looks at both the likelihood of something bad happening and the severity of that bad thing to determine which changes would be the most impactful.

"The government can say 'produce secure electric vehicle chargers,' but budget-oriented companies don't always choose the most cybersecure implementations," Wright said.

"Instead, the government can directly support the industry by providing fixes, advisories, standards and best practices. It's impossible to create solutions if you don't understand the state of the industry. That's where our project comes in; we did the research to find where we are and what gaps would be the quickest and most impactful to fix."

**More information:** Jay Johnson et al, Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses, *Energies* (2022). DOI: 10.3390/en15113931

Provided by Sandia National Laboratories

Citation: Vulnerabilities of electric vehicle charging infrastructure (2022, November 15) retrieved 25 April 2024 from https://techxplore.com/news/2022-11-vulnerabilities-electric-vehicle-infrastructure.html